EXHIBIT 54

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF J. ALEX HALDERMAN IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

Georgia's Current Election Technology

2. Georgia recently deployed new voting equipment and software manufactured by Dominion Voting Systems, Inc. ("Dominion"). These components include ImageCast X Prime ("ICX") ballot marking devices ("BMDs"), ImageCast Precinct ("ICP") precinct-count scanners, ImageCast Central ("ICC") central-count scanners, and the Democracy Suite election management system ("EMS"). Georgia

Secretary of State Brad Raffensperger certified these components in August 2019,[1] and they were first used statewide during the June 20, 2020 election.[2]

3. Under this new system (the "BMD-based Election System"), Georgia generally requires all in-person voters to select candidates on Dominion ICX BMDs. These devices are computer tablets connected to off-the-shelf laser printers. They do not record votes but instead print paper records that are supposed to contain the voter's selections in both human-readable text and as a type of machine-readable barcode called a QR code. Voters insert these printouts into Dominion ICP optical scanners, which read the barcodes and count the votes encoded in them.[3]

4. Absentee voters do not use BMDs but instead complete hand-marked paper ballots ("HMPBs"), which are tabulated at central locations by Dominion ICC scanners. While Georgia's precinct-based ICP scanners have the capability to count hand-marked paper ballots,[4] the State only uses them to count BMD printouts.

---

[1] Georgia Dominion certification (Aug. 9, 2019), https://sos.ga.gov/admin/uploads/Dominion_Certification.pdf.
[2] Mark Niesse, "How Georgia's new voting machines work," *The Atlanta Journal-Constitution* (June 9, 2020), https://www.ajc.com/news/state--regional-govt--politics/how-georgia-new-electronic-voting-machines-work/RyIOJuHYQgktcCNGL9sEoK/.
[3] Decl. of Dr. Eric Coomer, Dckt. 658-2, at 10.
[4] *Id* at 9.

5. Pre- and post-election procedures in the BMD-based election system closely parallel those under the old DRE-based election system. Before every election, the Secretary of State's office prepares election programming files using Dominion EMS software, which is a collection of client and server programs that run on commercial-off-the-shelf (COTS) computers and servers. The Secretary of State transmits the election programming files to county officials, who use another instance of the Dominion EMS to prepare memory cards and USB sticks for every scanner and ballot marking device used in the county. These removable media contain the ballot design, including the names of the races and candidates, and rules for counting the ballots. Election workers install a memory card or USB stick into each BMD and ICP scanner prior to the start of voting.

6. After polls close, election workers remove the memory cards from every ICP scanner and return them to the county. At that point, the memory cards contain a digital image of each scan as well as the scanner's interpretation of the votes contained in the barcode. County workers use the Dominion EMS to retrieve data from the cards and prepare the final election results based on the barcode readings.

Attacks Against the BMD-based Election System

7. Attackers could alter election outcomes under Georgia's BMD-based election system in several ways:

(a) Attacks on the BMDs could cause them to print barcodes that differ from voters' selections. These changes would be undetectable to voters, who cannot read the encrypted barcodes. Since the barcodes are the only thing the scanners count, the impact would be a change to the election results. The only known safeguard that can reliably detect such an attack is to rigorously audit both the human-readable portion of the printouts and the barcodes, which Georgia does not currently do.

(b) Attacks on the BMDs could also change *both* the barcode and the human-readable text on some of the printouts. Research shows that few voters carefully review their BMD printouts, and, consequently, changes to enough printouts to change the winner of a close race would likely go undetected. No audit or recount could detect this fraud, since both the digital and paper records of the votes would reflect the same selections but not the ones the voters intended.

(c) Attacks on the scanners could also cause fraudulent election results by changing the digital records of the votes. The only known safeguard that can reliably detect such an attack is a sufficiently rigorous manual audit or recount of the paper records, which Georgia does not currently require.

state, in the same way that malware could have spread through the old DRE system, which was not effectively air-gapped or otherwise reasonably secured.

10. The BMD-based election system is at further heightened risk of attack because of the legacy of poor security in Georgia's old DRE-based election system and its associated computers and networks. If attackers infiltrated the DRE-based system, they likely did so by first infiltrating components such as the Secretary of State's computer network, the voter registration database software developed by PCC, Inc., or the non-"air gapped" computers and removable media used by state and county workers and outside contractors to transfer data into and out of the EMS. The record in this matter contains abundant evidence about vulnerabilities in all these components, some of which were unmitigated for years and may still be unmitigated. Responsibility for their security continues to rest with many of the same technicians and managers who oversaw the security of the old system and were unable or unwilling to implement effective security measures.

11. These components continue to be used with the new voting system, including to process data that is copied to polling-place equipment. If attackers breached any of them to attack the DRE-based system, those attackers may continue to have such access under the BMD-based system. Technologies that the State has highlighted as key defenses for these legacy components, such as anti-malware

scans, anti-virus scans, and endpoint protection, provide little defense against sophisticated attackers like hostile foreign governments.

12. Importantly, apart from the examinations Fortalice conducted that found significant vulnerabilities with the Secretary of State's information technology infrastructure including components of the election management network, there is no indication that Georgia has ever forensically or otherwise rigorously examined the current election system, including components from the prior DRE-based system that are used with the current BMD-based system. In an environment of advanced persistent threats to both election systems, coupled with the critical known vulnerabilities with those systems, the lack of any such examination raises serious concerns about the reliability of the current system and election outcomes.

Georgia's New Dominion Equipment has Critical Security Flaws

13. Dominion does not dispute that its products can be hacked by sufficiently capable adversaries.[6]

14. One reason why this is true is the complexity of the software, which far exceeds the complexity of the DRE-based system. The Dominion software used in

---

[6] Decl. of Dr. Eric Coomer, Director of Product Strategy and Security for Dominion ¶ 13, Dckt. No. 658-2 ("all computers can be hacked with enough time and access").

24. Furthermore, the California testers found that the Dominion system's antivirus protection was insufficient or non-existent. "[O]n the EMS server, the AVAST Antivirus (AV) File Shield (the real time AV monitor) was only able to detect and clean one of the four [test] files. This potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text."[23] Moreover, the ICX BMD and ICP scanner have no antivirus software at all.[24] As a result, malware that infected the Dominion components could evade antivirus detection.

25. One of the ways that attackers might affect election equipment is by physically accessing the devices. In the case of the Dominion BMD, the California source code reviewers found a vulnerability that can be exploited with physical access to the USB port that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider."[25] This implies that no passwords or keys would be needed to exploit the problem, given physical access. California testers also found that "the ICX device does not provide monitoring of

---

[23] *Id*. at 19-20.
[24] *Id*. at 20.
[25] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019) at 29, https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.

increases the "attack surface" of the election system: with two potentially vulnerable components to target instead of just one, attackers are more likely to succeed.

30. Georgia's Dominion ICX BMDs are computers, they run outdated and vulnerable software, and they must be programmed using the State's election management system before every election. Attackers could potentially infect Georgia's BMDs with malware in several ways, including by spreading it from the election management system (EMS).

31. An attacker who infected the BMDs with malware could change a fraction of the printouts so that the barcodes encoded fraudulent votes but the human-readable text showed the voters' true selections.

32. Voters would have no way to detect this attack. They cannot read the Dominion barcodes, which are encrypted, so it is impossible for them to verify whether the barcodes really match their selections. However, when the Dominion scanners tabulate BMD printouts, they ignore the printed text entirely and count only the votes encoded in the barcodes. This means that voters cannot verify the portion of their ballots that gets counted.

results. If the discrepancies resulted from an attack, this would cast doubt on *both* the barcodes and the ballot text. An attacker who was able to alter the barcode would be equally capable of altering the ballot text. Malware might be designed to sometimes alter only the barcode and sometimes only the text. This means that officials could not simply ignore the barcodes and count only the text if they suspected the BMDs had been compromised.

37. BMDs do not need to use barcodes. Several kinds of modern, EAC-certified BMDs deployed in other states do not use barcodes to encode votes. These include the Clear Ballot ClearAccess system[34] and the Hart Verity Touch Writer.[35] Instead of a barcode for vote tabulation, these systems print a ballot that looks like a hand-marked paper ballot but has scan targets filled in for the selected candidates.

38. In Dominion's response to the State's request for proposals, the company represented that an upcoming version of its BMD software would not need to print barcodes on ballots.[36] Instead, the BMDs would produce (and the scanners

---

[34] *See* Clear Ballot, "ClearAccess Accessible Voting," https://clearballot.com/products/clear-access.
[35] *See* Hart Intercivic, "Verity Touch Writer Ballot Marking Device," https://www.hartintercivic.com/wp-content/uploads/VerityTouchWriter.pdf.
[36] "Clarification Questions\MS 16-1 Supply Chain_Dominion and KNOWiNK Final.docx" *available at* https://sos.ga.gov/admin/uploads/Dominion.zip (last visited Aug. 19, 2020).

would count) an entirely human-readable ballot capable of verification by the voter. However, this option is described as an "upgrade" available only after "certification is complete at the EAC."

39. The Secretary of State's office and Dominion portray Georgia's BMDs as having this ability to print such a human-readable, "full-face" ballot. A video portraying such a capability is part of the "Important Voter Information" available to the public on the Secretary of State's elections security web page.[37] The video portrays a voter making her selections on a BMD displaying a mock ballot using Georgia state and local races and constitutional questions or referenda. At the end of the video, the voter selects "Print Ballot," and the attached printer produces a double-sided ballot with a darkened oval appearing next to the voter's selections.[38]

40. Dominion's in-precinct optical scanners already are capable of and certified to read such full-face paper ballots that do not encode votes using barcodes.

---

[37] https://www.dropbox.com/s/u0lc21u82ye2qpg/ICX%20BMD%20Cart.mp4, available through "Voting Cart" hyperlink at https://sos.ga.gov/securevoting (last visited Aug. 18, 2020).
[38] *Id.*

BMDs Limit the Effectiveness of Voter Verification

41. Even if Georgia were to implement rigorous post-election audits, BMDs make it possible for an attacker to compromise the auditability of the ballots and thereby undermine the primary goal of the paper trail. To do so, malware would cause the BMDs to sometimes print fraudulent selections in *both* the barcode and the human-readable text. This attack would be impossible to detect by auditing the printouts, because all records of the voter's intent would be wrong. Pre-election testing and parallel testing also cannot reliably detect such cheating.

42. Unlike the security of hand-marked paper ballots, the security of BMDs relies critically on voters themselves. The only practical way to discover a BMD attack that altered both the barcodes and the printed text would be if enough voters reviewed the printouts, noticed the errors, and alerted election officials. Yet several recent studies, including my own peer-reviewed research, have concluded that few

voters carefully review BMD printouts.[39,40,41] As a result, the BMD paper trail is not a reliable record of the votes expressed by the voters, and changes to enough printouts to change the winner of a close race would likely go undetected.

43. Even if some voters did notice that their selections were misprinted, these voters would have no way to prove that the BMDs were at fault. From an election official's perspective, the reporting voters might be mistaken or lying. Many voters would need to report that the BMDs misprinted their ballots before officials could be sure there was a systemic problem.

44. There are no protocols or policies in Georgia that I have found that address how many voter complaints, or other conditions, involving BMDs would be required within or across polling places to support a finding—or even a robust investigation—of a systemic problem. Moreover, it would be virtually impossible

---

[39] R. DeMillo, R. Kadel, and M. Marks, "What voters are asked to verify affects ballot verification: A quantitative analysis of voters' memories of their ballots" (2018). Available at https://ssrn.com/abstract=3292208.

[40] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" in *Proceedings of the 41st IEEE Symposium on Security and Privacy* (Jan. 2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

[41] Philip Kortum, Michael D. Byrne, and Julie Whitmore, "Voter Verification of BMD Ballots Is a Two-Part Question: Can They? Mostly, They Can. Do They? Mostly, They Don't" (Mar. 2020), https://arxiv.org/ftp/arxiv/papers/2003/2003.04997.pdf.

any election, and an attack would likely not be detected if it occurred in a contest that was not the target of the RLA or during an election for which no RLA was conducted. Even for the one contest every two years that would be audited, the proposed rule does not describe the auditing procedure in enough detail to evaluate its sufficiency. The specific process that election superintendents would follow to carry out the audit is yet to be defined.

55. No matter what auditing procedures Georgia applies, the state's widespread use of BMDs makes it possible for an attacker to undermine the integrity of the paper trail. Malware could cause the BMDs to print fraudulent selections, both in the barcode and the human-readable text. Such an attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong.

Hand-Marked Paper Ballots Are Much More Secure

56. Hand-marked paper ballots (HMPBs) are the most widely used voting technology in the United States. More than 65% of voters live in jurisdictions that use HMPBs as their primary in-person voting technology,[48] and all 50 states, including Georgia, use them for absentee voting. When used with modern precinct-

[48] Verified Voting, *The Verifier*.

for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results."[56]

63. Georgia's BMD-based election system does not achieve the level of security necessary to withstand an attack by these sophisticated adversaries. Despite the addition of a paper trail, it suffers from severe security risks much like those of the DRE-based election system it replaced. Like paperless DREs, Georgia's BMDs are vulnerable to attacks that have the potential to change all records of a vote.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 19th day of August, 2020 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

[56] *Id.*